Will Deepfake Technology Defeat Biometric Authentication?

By Dean Nicolls | October 10, 2019

Deepfakes are everywhere.

From video impersonations to celebrity face swaps, they are becoming the modern-day meme because they're relatively simple to create. A deepfake superimposes existing video footage of a face onto a source head and body using advanced neural network powered AI. In other words, a deepfake looks to be a real person's recorded face and voice, but the words they appear to be speaking were never really uttered by them, at least not in that particular order.

While you may think you've never been fooled into thinking a deepfake was real, none of us can be 100% sure, because just like well-done special effects in a Hollywood movie, some are so good that we'll never even notice.

FACETEC EXHIBIT 2043
JUMIO v. FACETEC
IPR2025-00109

Researchers from cybersecurity company Deeptrace recently found 14,698 deepfake videos online, compared with 7,964 in December 2018. They said 96% were pornographic in nature, often with a computer-generated face of a celebrity replacing that of the original adult actor. Not surprisingly, deepfake technology is also being weaponized for political misinformation and cybercrime. Back in August, criminals used AI-based software to impersonate a chief executive's voice and demand a fraudulent transfer of $243,000. In that scam, the head of a UK-based energy company thought he was on the phone with his boss, the chief executive of the firm's German parent firm, who directed him to send the money to a Hungarian supplier. The German caller claimed the request was urgent and ordered the unwitting UK executive to initiate the transfer within the hour. Oops.

Enter, biometric authentication.

Now, think about the growing popularity of biometric authentication. According to Gartner, by 2022, 70% of organizations using biometric authentication for workforce access will implement it via smartphone apps. In 2018, the figure was fewer than 5%. So, an obvious question is whether deepfakes can fool these biometric-based solutions.

The answer: Some do and some don't.

I know that's not a very satisfying answer. But it genuinely depends on the type of liveness detection that is integrated into the identity verification solution.

So what is liveness detection and how can it sniff out deepfakes?

Many modern identity verification solutions now require new users to take a picture of their driver's license (or some other government-issued ID) and then take a corroborating selfie. The face in the selfie is then matched to the face on the ID document and a yes/no decision as to whether the person in the selfie is also shown on the ID is rendered. Seems pretty simple right?

Well, unfortunately, it's not.

A number of years ago, cybercriminals started using photos and pre-recorded videos to bypass biometric-based verification systems. In response, identity verification providers introduced different types of liveness detection to attempt to differentiate between real human users and spoof artifacts. The goal is to know if the biometric data being matched is from the live, physically present person at the time of capture. Put simply, liveness detection prevents bots and bad actors from using photos, videos, masks or other biometric data (stolen or otherwise) to create or access online accounts. Liveness ensures only real humans can create and access accounts.

Sometimes liveness detection methodologies ask users to blink, smile, turn/nod, watch colored flashing lights, make random faces, speak random numbers and much more. Sadly, most of these legacy techniques are easily spoofed by deepfakes.

Digital Trust Throughout the Customer Journey

How to Leverage the Jumio Platform from Onboarding to Ongoing Monitoring

Get the Guide

Enter, certified 3D liveness detection.

In the world of liveness detection, there is a large distinction between certified and uncertified methods. Certification testing is performed by iBeta, a NIST/NVLAP-accredited lab, based in Denver. They are currently the only lab performing presentation attack detection (PAD) testing guided by the all-important ISO 30107 global standard.

In fact, Jumio is proud to have partnered with FaceTec, which recently received perfect scores in testing guided by the ISO 30107 biometric standard. FaceTec is the first and only biometric technology to achieve perfect results in Level-1 and Level-2 certification testing. This is noteworthy because the Level-2 test attempts to spoof the technology even using live human test subjects wearing realistic 3D masks.

Between the two levels of certification, FaceTec successfully stopped more than 3,300 spoof attempts over the course of 12 days of rigorous testing. Artifacts and masks used for sophisticated attacks include digital and paper photos, high-resolution video, lifelike dolls and realistic latex masks, according to the iBeta testing documentation.

Like a high-stakes game of whack-a-mole, when the fraudsters try to emulate a real human with one spoof method they expose different non-human traits that the AI picks up on. In this case, at their core deepfakes are 2D videos, not 3D human faces, so they become relatively easy to discern for a certified 3D liveness detection provider like FaceTec. The computer monitor used to play back the video emits light — it doesn't reflect it — and certified liveness detection can tell the difference. And, if a criminal attempts to use the deepfake video with a projector onto a 3D head, then the skin texture won't be quite right, and the advanced certified liveness solution will detect the generation loss, a surefire tipoff.

As it turns out, iBeta's PAD Level 1 test has an ISO 30107-3 requirement called "Cooperative User/Tester." This means the testing simulates a user being complicit in the fraud or someone who has their biometric data phished unknowingly. So, just like a complicit user would, the test

subjects provide “any and all” biometric data requested by the testing organization. This makes the iBeta PAD test significantly more difficult than tests that only leverage publicly available biometric data or non-cooperative subjects. The goal is to ensure the authenticator’s liveness detection is strong enough to combat complicit user fraud, synthetic ID fraud and even phishing attacks.

However, it is important to remember that not all liveness is created equal and many un-certified liveness detection solutions fall prey to deepfakes. In addition, puppets and avatars that rely on “challenge/response liveness systems” easily bypass many liveness checks because it’s easy to make the avatar to react to rote commands. Check out a video that FaceTec created in just a few seconds to demonstrate how criminals can use this type of cutting-edge software to dupe legacy liveness detection.

To even have a chance to sneak past certified solutions you’ll need to invest in expensive, bleeding-edge technologies. For example, you’d probably need a 3D animatronic puppet that could somehow exhibit a lifelike combination of reflections in the eyes, pupil reactions and a variety of very subtle movements as well as simulate real-looking eyelids, skin and hair texture, and facial contours. This requires a much bigger investment — not only in technology, but in time as well. This could cost millions of dollars and take months, if not years to master, and there is still no guarantee that it would work.

Modern organizations should rightfully be concerned about deepfakes and how they can be deployed to infiltrate your online ecosystem. That’s why it’s vitally important to embed 3D liveness detection into your identity verification and authentication processes, and equally important to insist upon a iBeta-certified solution that can withstand deepfakes and other advanced spoofing techniques.